NOTE TO DF-120 "REPORT ON THE SOLUTION OF MESSAGES IN DEPTH OF THE AMERICAN CIPHER DEVICE M-209".

Attention is called to the apparent discrepancy between the figure 33 appearing in figure 10 ($x \frac{100}{33} = 55.400$ etc) and the statement in the sixth line from the bottom of page 13. The division in the text calls for doubling the number of positions. This step in chart 10 is two operations, 33 being the actual number of positions. From the textual account it is obvious that "33" is the number to be doubled. E.C.

12 July 1948

25 copies: Copy No. 2
1 page.

Distribution:-

1	AS-10, AS-23, AS-14 file
2	AS-70, AS-76-C file
3	AS-80, AS-83 file
4	AS-90, AS-95 file
5	AS-96
6-7	CSAW
8-9	LSIC
10	CSGID
11	CBO
12	ASA/Europe
13	ASA/Pacific
14	ASA/School, Officer's Training Division
15	AS-93
16	AS-94
17-18	AS-80
19-20	AS-70
21-25	file

DF-120
TICOM Doc. 2794

58/48/TOPSEC/AS-14-TICOM

76 C File

REPORT ON THE SOLUTION OF MESSAGES IN DEPTH OF THE

AMERICAN CIPHER DEVICE M-209

1. The attached is an Army Security Agency translation of TICOM Document 2794, German title: "Bericht über die Losung phasengleicher Sprüche der amerikanischen Schlüsselmaschine M-209."

2. This is one of the reports of the Signal Intelligence Agency of the High Command of the German Army (OKH/GdNA/In 7/VI). As a result of information received by U.S. Military Intelligence Service, Austria, they were found buried in a camp at Glasenbach, Austria, and were forwarded through ASA/Europe to TICOM at LSIC in May 1947.

3. Considerable liberty has been taken in this translation (as was done in TICOM Doc. 2795, "Determination of the Absolute Setting of the AM-1 (M-209) by Using Two Messages with Different Indicators") in order to have the text conform to standard Army Security Agency usage. While the techniques described here are quite similar to those employed in related Hagelin type problems the presentation has been found to be clear and self explanatory. One of the statistical methods is interesting because of its probable application in other problems.

CSGAS-14-TICOM
23 June 1948
Translated: EC

No. of pages: 17
25 copies
Copy No. 2.

Distribution:-

1	AS-10, AS-23, AS-14 file
2	AS-70, AS-76-C file
3	AS-80, AS-83 file
4	AS-90, AS-95 file
5	AS-96
6-7	CSAW
8-9	LSIC
10	CSGID
11	CBO
12	ASA/Europe
13	ASA/Pacific
14	ASA/School, Officer's Training Division
15	AS-93
16	AS-94
17-18	AS-80
19-20	AS-70
21-25	file

REPORT ON THE SOLUTION OF MESSAGES IN DEPTH OF THE AMERICAN CIPHER DEVICE M-209

A. Introduction: General Remarks

Today I have the task of giving you a short survey of the work which is being accomplished in Section 2a on the American Cipher Machine M-209. The work in our section is restricted exclusively to the purely linguistic solution of such machine messages, while the reconstruction (possible on the basis of such linguistic solution) of the internal setting of the machine, which is valid for the day, is taken up in Section 1b. I should like for that reason here to restrict myself to the purely linguistic aspects and therefore to mention to you only so much of the basic construction and method of operation of the machine as is absolutely necessary for you to follow my presentation.

First of all a few words about the machine itself. It is, essentially, a machine of the Hagelin type, which is known by the Americans under the title M-209, but is known by us either as AM-1 or BC-38. It was produced in Sweden. The machine belongs to the same type as the already well-known BC-36, and follows the same cryptographic principle. I will not explain here in detail the basis of this principle; let me just remark (because this is important for linguistic solution) that it is a matter of encipherment by means of polyalphabetic substitution, i.e., each letter of a message is enciphered with a different substitution. The machine is so built that a repetition of the same substitution sequence appears only after 101, 405, 850 substitutions. This number corresponds to the product of the lengths of the 6 keywheels in the machine, whose lengths are 26, 25, 23, 21, 19, and 17 letters, and are prime to each other. On the 26 wheel all the letters of the alphabet are represented; on the 25 wheel "W" is missing; on the 23 wheel

"W, X, Z" are missing; on the 21 wheel "V, W, X, Y, Z" are missing; on the 19 wheel "T, U, V, W, X, Y, Z" are missing; and on the 17 wheel all the letters from "R to Z" are missing. With a daily change of the internal setting a solution of messages enciphered in this way would seem to be rather hopeless. One circumstance, however, gives us in certain cases the possibility of breaking in. The substitutions, which are effective at each individual position of the message, are alphabetical and reciprocal. That means that at each position in the message only one definite substitution out of a choice of 26 different ones is possible. These 26 different substitutions come about because a normal alphabet and a reverse standard alphabet have been slid against each other. (Compare the sliderule!) At any rate, we do not know which of these 26 different possible substitutions will be effective at any given position. However, when messages appear which were enciphered with the same internal and external setting of the machine--and this is apparent from the similarity of the indicator groups on the same day--a linguistic solution is possible. That is to say, if one superimposes two such messages, and if one knows at any given position the arrangement of the clear text letters in one of the two messages, one can determine, with the help of our slide, the clear text letters for the other message at this position. How one utilizes this fact in solution I will show more clearly in the course of my remarks.

First, however, permit me a few more general remarks. The first use of the machine by the Americans occurred in December 1942 in the African theater of war. The messages are recognizable through two 5-letter indicator groups at the beginning of the message of the type AABCD EFGXY, which are repeated at the end of the message, mostly in the same order, but also sometimes reversed. At another place I will go into more detail concerning the meaning of the indicators. The first messages in depth, that is, messages with like indicator groups, appeared in January 1943. Since it was a matter of exceptionally long messages of 682 letters, the entry into the entire system succeeded with them. The two messages were linguistically solved and the first internal machine setting found analytically.

When in April and May 1943, the then widely used strip system, known as M-94 or URSAL strip, was supplanted by this machine, we could read this new traffic currently as long as messages in depth appeared. Thus, messages were solved from the theater of war in Africa, later in Sicily, and Italy, and also from the Anglo-American invasion army which was waiting in England. Here it was mainly a question of practice messages, which, nevertheless, were read currently and which gave valuable hints to Evaluation,* so that, by the beginning of the invasion, a rather clear picture of the strength and composition of the invasion army had been built up. Since the beginning of the invasion messages mainly from the Western front and from Italy are being worked on.

The internal setting of the machine is valid for a definite key area and is changed daily. According to regulations, the indicator group and, with it, the external setting of the 6 key wheels, is supposed to be changed from message to message, but fortunately this is not always done, for, otherwise, no messages in depth would appear at all.

The machine is used principally for the encipherment of tactical messages from division down to, and including, battalions. Sometimes, however, even the corps use it.

* (It should be noted that in German Signal Intelligence practice Evaluation is distinct from Traffic Analysis and corresponds closely to the British "Fusion".)

B. Solution of Messages in Depth.

1. Strip Method.

Following this introductory survey I should like to proceed to a discussion of the methods of the actual linguistic solution. If you will please recall what I said at the outset: viz., if I know the clear text at any position in one of two messages in depth, then, with the help of our slide, the clear text at the same position of the second message is very easy to reconstruct.

Here I shoul like to explain in passing just how we came by this slide. (See Figure 1.) The illustration shows the type of wheel of the machine with the two reciprocal alphabets. In enciphering, the clear text letters are put in on the left hand alphabet, the machine is operated and the right hand alphabet writes the cipher letters corresponding to the internal setting of the machine at the time. Our slides, then, are nothing more nor less than these two circular alphabets unrolled and set next to each other as strips which can be slid against each other. Thus, if we know the relationship of clear-cipher at one position, the slide immediately furnishes us with the entire substitution alphabet which is effective at this position. This fact can be exploited in the following manner: a word suspected to appear in one message --for example, a number--can be set down at all positions of the message and, at each position, corresponding clear text in the other message can be sought. If the suspected word is actually at any position in the message, then, at the same position in the second message, a fragment of clear text must appear. This method, however, is very bothersome and time wasting. Therefore, we have attempted the simplification which follows. (See figure 2.)

Let us assume that at all the positions of the first message the clear text letter "Z" appears and see which clear text letters correspond to it in the second message. We do the same for "A", "B", and "C" and so forth. These corresponding letters we write under each other in columns, above which, as a heading, we write the letters of the alphabet with which we had begun. As you will see, by no means does this have to be done for all the letters of the alphabet, but, whenever one has a complete column, one can obtain the other letters by alphabetical progression. The completed strips are then cut apart and used in testing for probable words in one message. (For example, the word THREE.) The Z-strip is made in duplicate since "Z" can be tried as a separation letter before and after the suspected word. In order that the clear text expected in the second message will appear in a line the trial must be built up step-wise. (Compare figure 3.) If you find clear text, or fragments of clear text, in the second message, you count the lines from the top down, and obtain thereby the exact position in the message where the texts occur. Now, with the help of our slide, you can try, alternately above and below, to build up further text. If the trial hits and is not a coincidence, then, in building up further alternately above and below, clear text will have to appear.

We have obtained the following by this method: by one trial of a word we can see at a glance whether this word actually occurs at any position of the message.

Further, it has been shown to be very practical to use the same strips in reverse procedure, that is, to try in the second message all the letters of the alphabet and after the other and to write down the corresponding letters of the upper message in columns, one under the other. Then all we have to do is to turn the strips around and we can try the same probable work in the other message.

Strip writing by hand, especially for long messages, is a very tedious and time-wasting job, so we look for a method of doing it mechanically. A very practical solution is the strip writer (invented by Ofu. POKORN*) which is based on the following principles:

In a case of messages in depth, the interval between the two cipher letters is the same as the interval between the upperlying clear text letters, only with reversed sign (algebraic). (See figure 4.) U - D has the interval 9. If we put a "Z" against a "U" we must put a "Q" against the "D". Z - Q has the interval "minus 9". So now we have only to write two similar alphabets (this time not reciprocal!) under each other so that the letters which have an interval of 9 are above each other, being sure that the cipher relationship U - D corresponds to the clear text relationship Z - Q, only again in the reverse direction. We exploit this fact. We devise two slides upon which the alphabets are written in the same direction. The outer slide is fixed in such a way that the letter "Z" is at the bottom. Now you must turn the inner slide so that the cipher letter of the first message is set above the cipher letter of the second message, that is, above "D". Opposite the "Z" of the outer slide, then, always appears the clear letter which would correspond to a "Z" at this position of the first message. Thus we have, in order, the letters of our "Z" strip. With the inner slide, fastened tight, there is a type wheel which carries type slugs corresponding exactly to the inner slide, and one only has to draw type wheel across towards the right in order to obtain the alphabet beginning with the clear text letters of the

* (N.C.O., or Underofficer, Alfred POKORN was a cryptanalyst attached to the American Hagelin Section of In 7/VI of OKH. See TICOM I-175.)

"Z" column. Thus, to a certain extent, the apparatus combines into one process the actual writing of the alphabets and the seeking of the initial letter of each line appearing in the "Z" column. (See figure 5 and 6).

2. Bigraphic Frequencies.

Now back to the text. It often occurs that the alternating construction of clear text cannot be continued as far as desired, but that a place is reached where, both above and below, a word ends and so a "Z" appears in both messages. One can then guess what follows and try to build up further text as before. If that does not succeed, one can renew the trial of probable words without strips and, in this way, try to obtain a new break-in at another point. If that is not successful either, there is still a third method of making progress, that is, the so-called Bigraph Frequency. (See figure 7.) The name itself reveals its nature. At the point following the "Z" in both messages a new word has to begin. So we seek out in the next two positions all the bigraphs which could yield, in both messages at the same time, possible English words or good abbreviations. For this purpose we devise special strips. First of all we try, at the first position in one of the two messages, all of the letters of the alphabet, and we write this alphabet on a strip, and under each letter we write, in RED and displaced a little to the right, its corresponding letter from the second message. Do the same thing for each succeeding position. Then we begin to move the second strip past the first one, seeking out, in one line, all the positions which give possible English clear text bigraphs for both the red and black letters. Alongside these we then build up, with the next strip, a third letter, then the fourth, and so on. In this way we must at last, come upon the correct continuation if there is no garble--in which case one would not be able to find the correct bigraph. If one has found the continuation, the further building up proceeds as described above.

3. Text Offset by One Place.

With certain provisions there is still another possibility of attaining very quickly a solution of messages in depth, and that is when messages appear which completely agree in the first cipher groups. In such a case the same text must have originally been in both messages. At some position, then, this agreement of the cipher text ceases. If it is not a case of a cipher mistake (garble) or omission of letters or groups in the cipher text, then at this position the clear text of the two messages must become divergent. It may be that the continuing text, following a stereotyped beginning, is completely different in the two messages. Then our strip method must be used for solution. Often, however, farther on in both messages there is similar text, except that, at the breaking-off point in one of the two messages, a letter was omitted or mistakenly added, so that now the clear text in the two messages appears off-set by one. If such is the case, there is a very simple method of reconstructing this off-set clear text. (See figure 8.)

Let us assume that at the first position after the parallel there was an "A" in the upper message, then this would correspond to "D" in the lower message. Now, if the upper message, with respect to the lower one, is offset one place to the right, the "D" would have to appear again in the upper message in the next position, and the "P", which corresponded to it in the lower message, must appear at the third position above, etc. However, since any letter of the alphabet could have stood in the first position above instead of the arbitarily assumed "A", we must carry through the same method for all the letters of the alphabet. Since for "B", "C", etc., one always gets the letters which follow it in the alphabet, one has only to write the rest of the alphabets, column-wise down, and clear text must be found in one of the 26 rows. In our example, either in the upper message a double "Z" has been sent, or in the lower message the separation "Z" was forgotten. According to experience the sending of a double "Z" occurs most often. So, in the trial of an off-set by one, one will always begin by trying a "Z" at the first position after such parallels in the upper or lower message, then one gets the correct clear text immediately and saves oneself the trouble of writing down the alphabets. For the other case, we have set up a table on which the alphabets have already been written down so that we have only to bring them into the correct position in order to seek out the clear text from one of the 26 rows. The question arises how is a garble (transmission garble) made noticeable in this method? Naturally, in the line of clear text which we have found, the text stops at this position, but it just jumps over to another line. Not only that, but the interval or jump, from the original line is just as much as the garbled cipher letter is different from the correct one. In our example we assumed the garble "Q" instead of "O" and we see that the clear text jumps up exactly two lines further on.

4. Offset by Two.

A quite similar system can be employed in the case of a suspected offset of two in two similar texts. It can easily occur that, through a second error which works in the same direction as the first, a message is offset by one letter further. (See figure 9.) In this connection one must consider the following: the letter of the lower message which corresponds to the clear text letter tried in the first position of the upper message does not appear again until the third position in the upper message; the letter corresponding to this one occurs at the fifth position, etc. With that method we obtain, by alphabetical continuation, a kind of a grid. Furthermore, with an offset of two, the second, fourth, sixth, etc., letters stand dependent on each other, so one can use this method for them also, thereby obtaining a second square which can be interlocked, step by step, into the first one. After every step one must test the 26 lines which come out against the clear text, therefore 26 x 26 lines in all. In one of these 676 rows we must find the desired clear text. Naturally this system can be extended at will for offsets of 3, 4, 5, etc., but that becomes too complex and time-wasting, so one works more quickly and surely with out strip method.

Furthermore, with an offset of one or two only a short fragment of clear text needs to be tested in this manner, since, with only the help of our slide, one can build further without any trouble up to the point where either a garble or a new offset appears.

5. Depth: When the Double Letter in the Indicator Group is Different.

Now there is one other case to be discussed, one in which the messages in depth are not obtained until later, that is, when two messages are available in which the indicators agree except for the doubled letter. In order to make the following understandable to you, I must insert a few short words concerning the meaning of indicator groups and the enciphering technique of the Americans.

The ten letters of the indicator groups have the following meaning. The last two letters (XY) denote the cipher area or cryptosystem net in which the key in question is effective. The six letters from the third to the eighth position (the third group) indicate the basic setting of the six key wheels. They are to be chosen arbitarily by the radio man, but of course they must be within the scope of the wheels. The double letter in the first two positions (of the first group) serves to encipher this basic position and is also to be chosen arbitarily by the radio man. This double letter is enciphered 12 times with the basic setting and the first six usable letters which come out of this encipherment then give the real starting position of the six key wheels. Only with this setting can the message be deciphered.

Example. In enciphering the double letter "A" twelve times, the letters R B Z D X H M F Q T A S might appear. The initial setting of the machine for the message to be deciphered would then be R B D H M F, since the letter "Z" does not appear on the 23 wheel, and the letter "X" does not appear on the 21 wheel, and therefore these must be strickened out.

Now if we have two messages in which the indicator groups agree except for the doubled letter--for example in one of them the double letter is A and in the other one it is B--then under certain circumstances we can, by sliding the messages against each other, obtain the genuine messages in depth. That is to say, if the encipherment with the double letter "A" gave the letters as above, then the encipherment of the double letter "B" will give the letters which proceed them in the alphabet, or therefore, Q A Y C W G L E P S Z R. The initial settings of the two messages are therefore R B D H M F and Q A C G L E. Now, if you set the machine at the initial setting of the second message and encipher a letter, each one of the six key wheels will move forward one step, that is, one letter farther along in the alphabet. So, thereby, the exact initial setting of the first message is arrived at and the two messages are in depth from this point on. Thus, in this case, we obtain messages in depth if we omit the first position of the message with the double letter "B". In the case of an offset from A to C, we would have to omit two letters, and in the case of an offset from A to D, three letters, etc.

However, one point must be considered in this connection. The depth in the messages could appear because one letter had to be struck out (of the encipherment of the doubled letters) of our two encipherments at the same positions. If this is not the case, then we do not get any messages in depth.

Example. Let us assume that in the encipherment of the double letter "A" we would obtain the following series of letters: R B W D X H T F Q T A S. Then the encipherment with B would be Q A V C W G S E P S Z. Now the initial settings of the two messages would be as follows: R B D H F Q (W X T had to be thrown out), and Q A V C G E (W and S had to be thrown out). It will be seen that these two initial settings now have very little in common, namely, only the first two positions. In this case, naturally, no depth can be found by sliding the two messages against each other. It is illuminating that the probability of elimination of letters, which has to be done at the same position, becomes smaller and smaller the greater the distance the two doubled letters are separated from each other.

C. Criteria for Depth.

1. Trigraph Differences (See figure 10)

What has just been discussed covers the most important methods for recovering plain text from messages in depth. But very many of the messages with similar indicator groups, which come to us from the field stations, are not genuine messages in depth at all, but are messages with the same text which were enciphered twice in succession, since in the first encipherment a mistake was made in the setting of the machine. For this reason the real addressee could not decipher the message, sent a query back, and then the message was sent again with the correct encipherment. Linguistically such messages can, of course, not be solved. Often such messages can be recognized by their external appearance on account of a large number of doublets (vertical digraphs) in the two cipher texts, by the appearance of quite definite intervals between the cipher texts, with similar or almost similar length, with similar tactical times, while the intercept time usually is one or several hours apart. Often, however, it is not possible to decide in advance whether these are messages in depth or not, and therefore, a criterion has been sought which could give us a clue as to whether a pair of messages ~~are~~ is in depth or not. In doing that, as already explained above, the fact has been employed that the intervals between the cipher letters are exactly the same to each other as the intervals of the corresponding clear text letters--only with opposite signs.

From solved M-209 messages from Africa, out of 10,000 letters the 300 most frequent clear text trigraphs were counted (taking into account the separator letter "Z") and the clear text intervals of these trigraphs to each other were determined. The differences found correspond to the negative cipher intervals in messages in depth. The <u>triple number</u> (Zahlentripel) which arose was weighted with values built up simply from the product of the frequencies of their occurrences, since the probability that two definite clear text trigraphs will appear over each other is equal to the product of the frequency of the percentage of their occurrence.

From these differences a table was prepared which indicates for us the corresponding weight for every possible Zahlentripel. One now finds each interval triple which appears in the two cipher messages, in the upper as well as in the lower message, and adds up the weights which apply to them. The sum is then multipled by 100 and divided by twice the number of positions being investigated. It is multiplied by 100 in order to get a relationship to 100 positions, and divided by twice the sum of the investigated positions since we have looked up each position twice--once in the upper and once in the lower message. For this reason the different sign of the intervals for the clear and cipher text has no meaning. The final result then gives us a point of departure for telling whether the messages being investigated are in depth or not. Experience has shown that values of 50,000 or more make depth probable. Values under 40,000 speak against depth, and with numbers in between 40,000 and 50,000 one can count on either possibility. Of course, in doing this, scattering (Streuungen) and coincidences must be taken into account. These things can make a considerable distortion of the picture, especially in short messages. Nevertheless, up to now, we have, in general, been able to depend on the results, particularily in rather long messages.

2. Other Criteria

Other criteria by which depth can be determined are more of an external nature.

a. Number of Doublets. The doublet frequency of two English clear texts when a word separator letter is used is about 8%. In the cipher text of messages in depth, however, doublets occur only when there also are doublets at these positions in the basic clear texts. A doublet frequency of between 6 and 8 percent in our cipher text, therefore, signifies depth. This doublet criterion is not valid for messages which are offset by one in their clear text, since in this case doublets can occur only when two similar clear text letters follow each other, as for example, EE, SS, TT, etc. The expected value here is 2½%.

b. Different Length and Different Encipherment Times.

With the same length and the same encipherment time there is always the suspicion that we are dealing with the same text in both messages and that it was only sent one time wrong and one time correctly. Here we obtain, by means of our trigraph differences, a starting point for depth.

D. Difficulties in the Solution of Messages in Depth.

After all that I have said and shown to you up to now you could get the impression that the solution of machine messages in depth was a quite simple affair. But I have purposely chosen simple examples, which, furthermore, are all based upon genuine solutions of cases in which the individual methods lent themselves well to description. In conclusion I should like to show you another pair of messages of recent date which will demonstrate to you what difficulties one often has to overcome in solution.

There was the case of a pair of messages dated 15 December 1944 which was sent to us on 16 December 1944 by teletype from KOMA 7 in Italy. The length of the two messages was different, likewise the time of encipherment. The number of doublets was favourable. There was even a three parallel position, and the trigraph differences gave a calculation of 51,000 on 170 letters. All criteria, therefore, pointed towards depth. (See figure 11).

Within a very short time after preparing the strips, there were two unmistakable break-ins, (See red underline in figure 11) but there were not yet enough letters avialable in order to reconstruct the internal setting of the machine. We worked a whole day dragging through the message, without any success, frequent words from a list we had made ourselves. The short red position in the first line could not be built further and could, under certain conditions, be an accident. A digraphic frequency at the beginning was also unsuccessful. After the first break-in position there should come a proper name. It was, therefore, not suitable for a digraphic frequency. The second break-in was right at the end. A digraphic frequency from in front of it leading backwards also led to nothing, although we had at our disposal as an aid a dictionary which was arranged alphabetically backwards. So, there was nothing more to do than to keep on dragging through new words, and at last we succeeded in breaking in with the word FIELD. With that the other red places also fell apart immediately and now the internal setting of the machine could be reconstructed with relative ease.

After that the parts of the message which, up to then, had not been solved were easily read. One will admit further also that a solution, with the aid of our strips, by using proper names and infrequent words would hardly have been possible.

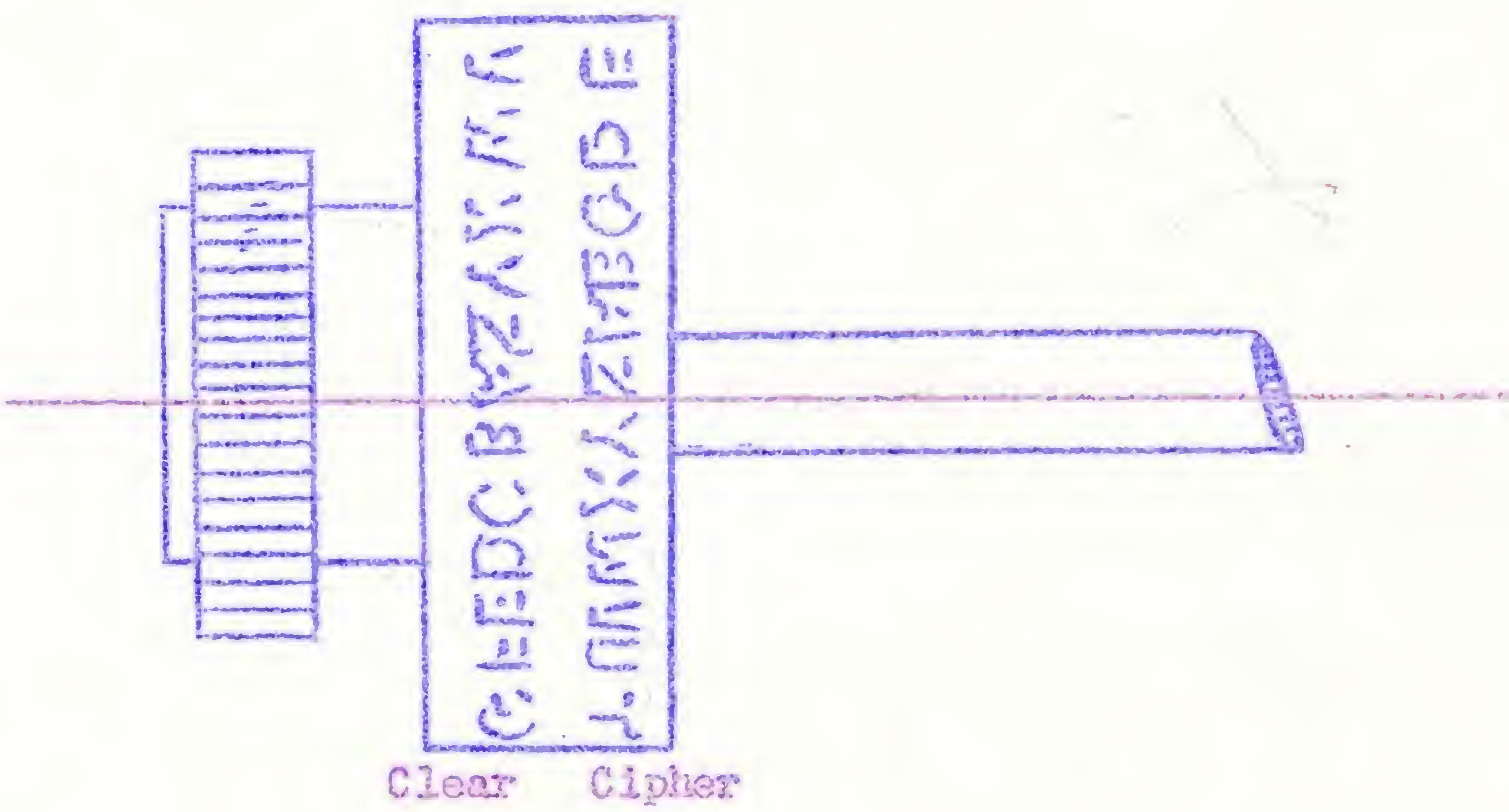
With this message the complications which the Americans attempted can be recognized. Stereotyped beginnings are, of course, forbidden, and likewise the encipherment of nulls by "X" or "Z" at the end of the message. They even have the messages begin in the middle of a sentence and then give the real beginning of the message somewhere in the middle. The beginning is made recognizable by the words MSG BGNS (message begins) or, as in our example, by a five-fold repetition of one letter. We have even had cases where at the beginning of a message only a part of a word appears; thus for example, "-sage", and the message then ends with the letters "mes-". With that, naturally, you can have no success from making a digraphic frequency at the beginning of the message. Another possibility, often used, is filling up messages at will at the beginning and at the end. After 5 to 10 nonsense letters the real message begins. Addresses are principally given only somewhere in the middle of the message, inclose either in the abbreviations PAREN, CMA, PD, CLN, OR XXX.

Further one must take account of many abbreviations, in the invention of which the Americans are great and completely unmethodical, and which can in themselves make the reconstruction of an already unknown text very difficult. After that there is always a sometimes greater, sometimes smaller percentage of garbles. But the most unpleasant thing is that now often even the numbers--our main source of entry--are not written out anymore but are

agreed M.E.W.

sent as doubled letters: 1 is aa; 2 is bb; 3 is cc;.....Ø is jj. And then when, as in this message, you add many personal names and infrequent words, the solution can often be very difficult. Then you have to have much patience, experience, and, added to that, a little bit of "fingertip feeling" in order to come to the desired success.

AM 1: TYPE WHEEL
RECIPROCAL ALPHABET



a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a

Figure 1.

MESSAGES IN PHASE.
BREAK-IN I.

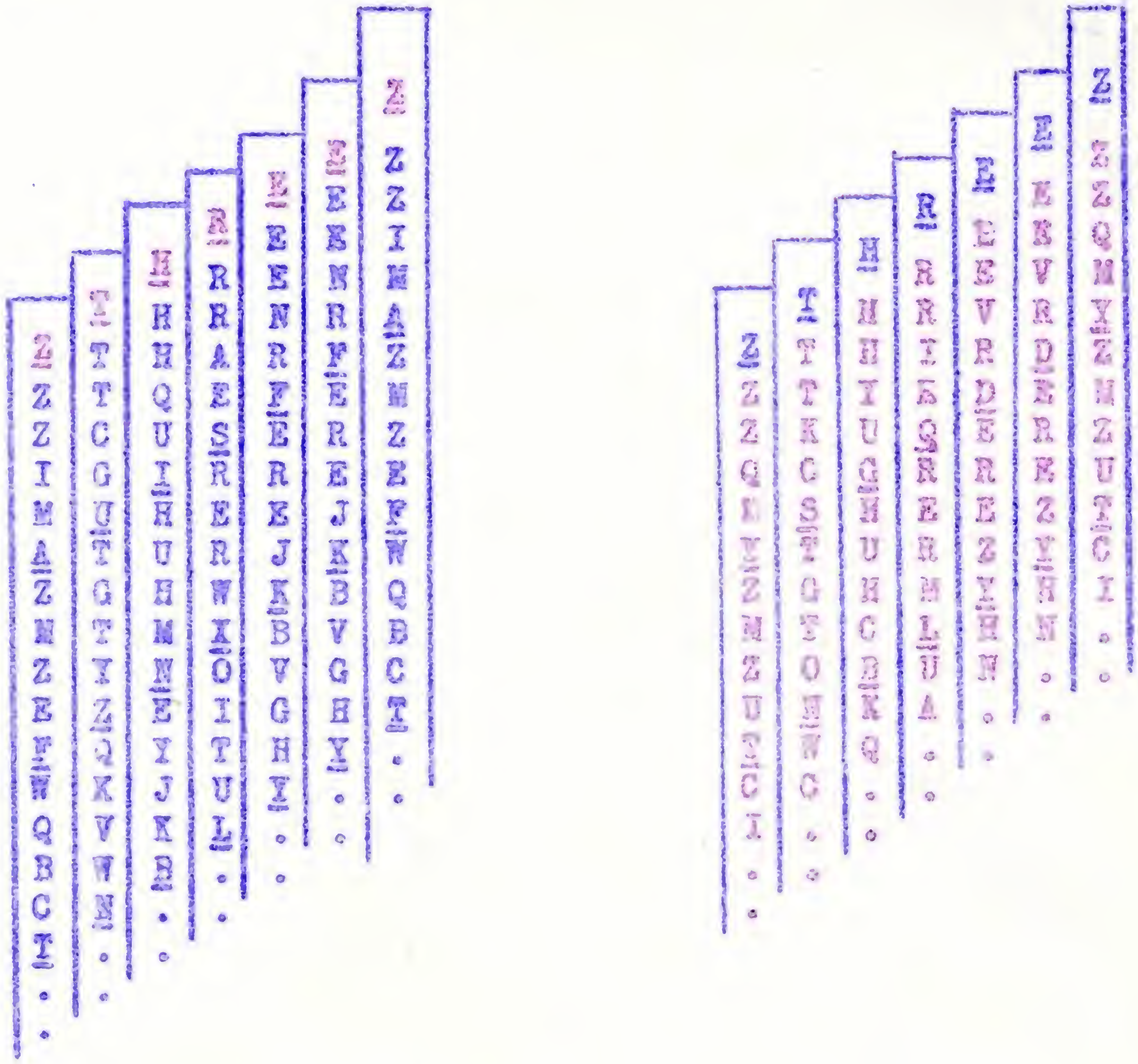
	.	.	.	.	.	.	.	.	.
	B	B	B	B	B	B	B	.	.
	A	A	A	A	A	A	A	.	.
	Z	Z	Z	Z	Z	Z	Z	.	.
MSG. 1	d	i	d	w	x	v	z	.	.
MSG. 2	d	i	u	j	w	v	m	.	.
	Z	Z	I	M	A	Z	M	.	.
	A	A	J	N	B	A	N	.	.
	B	B	K	O	C	B	O	.	.
	.	.	.	.	.	.	.	.	.

MSG. 1	MSG.2	Z	A	B	C	D	.	.
d	d	Z	A	B	C	D	.	.
i	i	Z	A	B	C	D	.	.
d	u	I	J	K	L	M	.	.
w	j	M	N	O	P	Q	.	.
x	w	A	B	C	D	E	.	.
v	v	Z	A	B	C	D	.	.
z	m	M	N	O	P	Q	.	.
z	z	Z	A	B	C	D	.	.
.	.	.	.	.	.	.	.	.

Z	T	H	R	E	E	Z
Z	T	H	R	E	E	Z
Z	T	H	R	E	E	Z
I	C	Q	A	N	N	I
M	G	U	E	R	R	M
A	U	I	S	F	F	A
Z	T	H	R	E	E	Z
M	G	U	E	R	R	M
Z	T	H	R	E	E	Z
E	Y	M	W	J	J	E
F	Z	N	X	K	K	F
W	Q	E	O	B	B	W
Q	K	Y	I	V	V	Q
B	V	J	T	G	G	B
C	W	K	U	H	H	C
T	N	B	L	Y	Y	T
.	.	.	.	.	.	.
.	.	.	.	.	.	.

Figure 2.

MESSAGES IN PHASE
BREAK-IN II.



```
         THIRD  .  .T  HREE.
MSG. 3.  didux  vzsqy  qxwps  qtjib  ggydd  ...
MSG. 2.  diujw  vmzls  tgumy  feyib  axduh  ...
         THREE  .  E.  EIGHT
```

Figure 3.

STRIP WRITING
EXPLANATION

MSG. 1 usltz . . .
MSG. 2 dxdtg . . .

						MSG. 1									MSG. 2						
CIPHER	.	.	.	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	. . .
CLEAR	.	.	.	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	. . .

← 9 →

						CLEAR				CIPHER									
9 ↓	.	.	.	n	o	p	q	r	s	t	u	v	w	x	y	z	a	. . .
	.	.	.	w	x	y	z	a	b	c	d	e	f	g	h	i	j	. . .

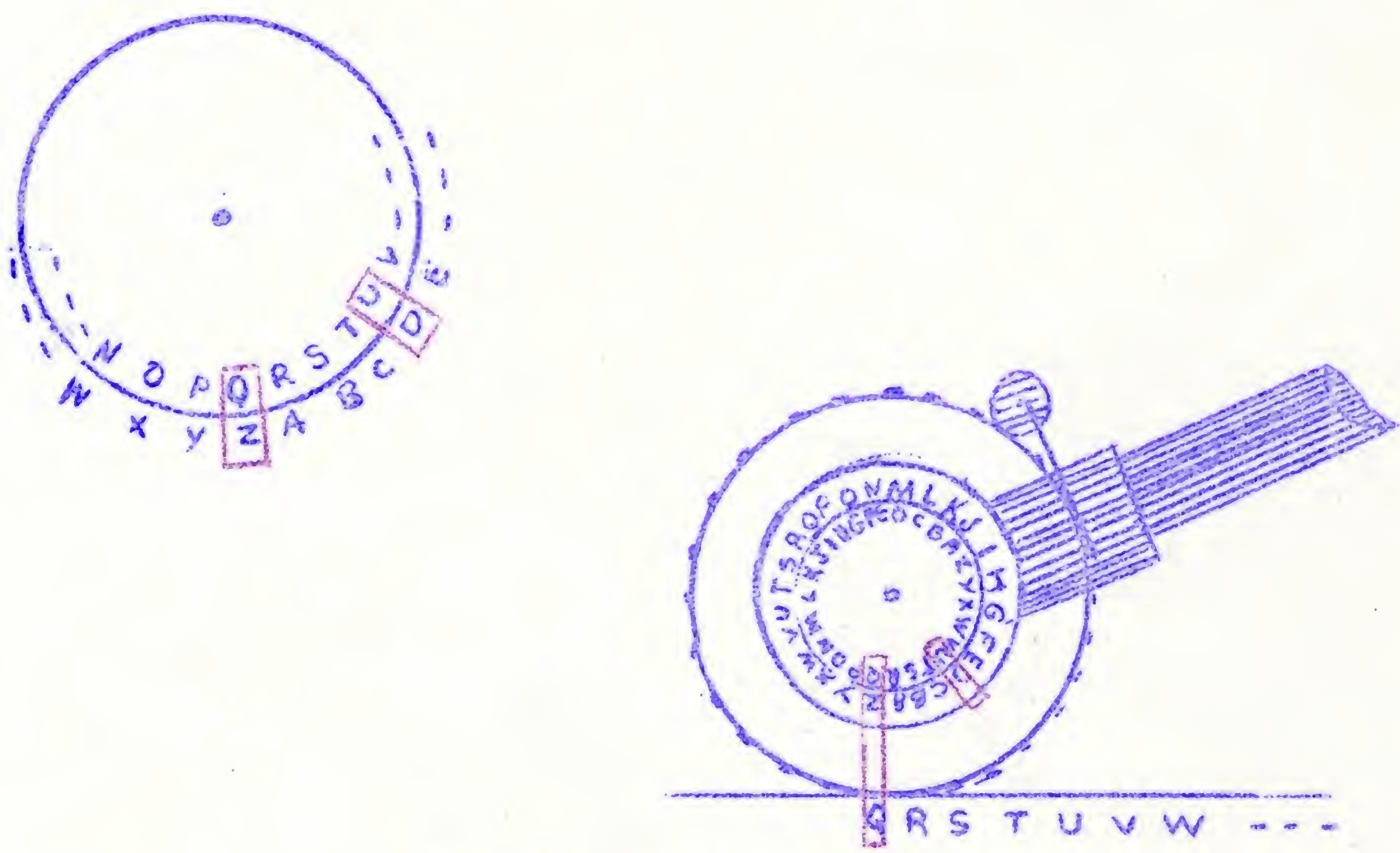


Figure 4.

STRIP WRITING

EXAMPLE I.

Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

Figure 5.

STRIP WRITING

EXAMPLE II.

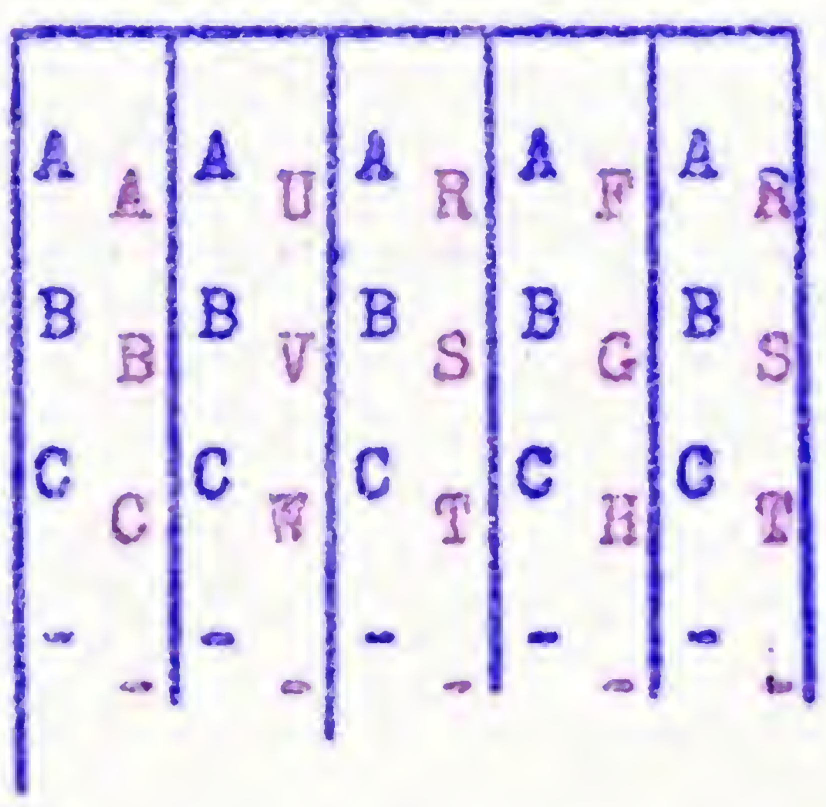
						Z
				E	E	Z
			R		E	Z
		H		E	E	I
	T		R	E	N	M
Z		H	R	N	R	A
	T	H	A	R	F	Z
Z	T	Q	E	F	E	M
Z	G	U	S	E	R	Z
I	G	I	R	R	E	E
M	U	H	E	E	J	F
A	T	U	R	J	K	W
Z	G	H	W	K	B	Q
M	T	N	X	B	V	B
Z	Y	N	O	V	G	C
E	Z	E	I	G	H	T
F	Q	Y	T	H	Y	K
W	K	J	U	Y	P	O
Q	V	K	L	P	T	
B	W	B	C	T		
C	N	S	G			
T	E	W				
K	I					
O						

Figure 6.

DIGRAPH- FREQUENCIES.

```
          . CP.
MSG. 1   feyib  axduh  ...
MSG. 2   otjib  ggydd  ...
          ONE.

          A  AAAA
MSG. 1    b  axduh
MSG. 2    b  ggydd
          A  URFR
```




```
          N  OW.I
MSG. 1    b  axduh
MSG. 2    b  ggydd
          N  INE.
```

2 Msg. of 26.10.44
ffacg nifus
2358 kHz

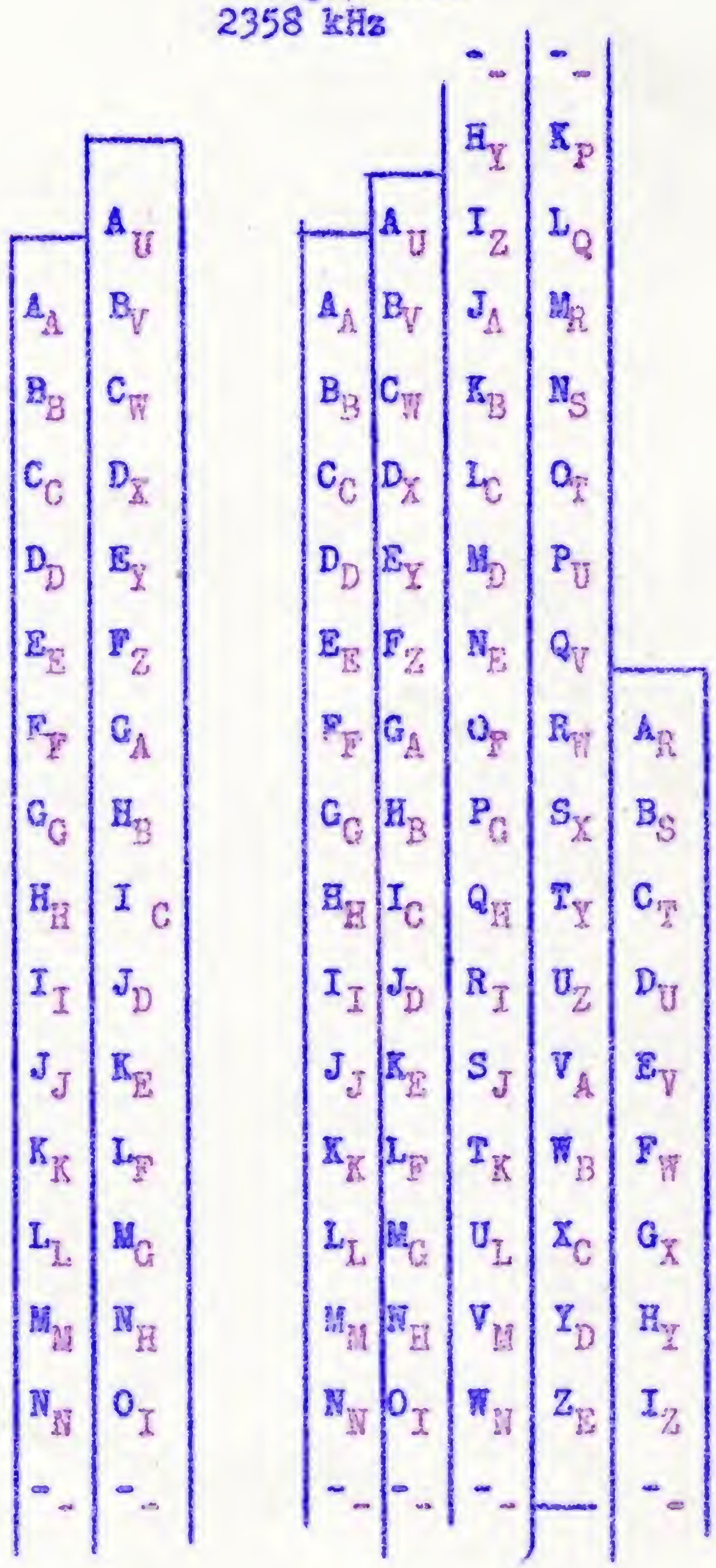


Figure 7.

OFF-SET OF 1

2 MSG. of 25.11.44
mmkof mfomm
2958 kHz

```
MSG. 1  slnug  ttbln  hxcfv  yliet  ...
MSG. 2  slnug  ttbib  vmoei  ipwvb  ...
```

```
         AD PBMAB O
MSG. 1  bln hxcfv y ...
MSG. 2  bib vmoei i ...
         DP BMABO E
```

```
DPBMABOE
EQCNBCPF
FRDOCDQG
GSEPDERH
HTFQEFSI
IUGRFGTJ
JVHSGHUK
KWITHIVL
LXJUIJWM
MYKVJKXN
NZLWKLYO
OAMXLMZP
PBNYMNAQ
QCOZNOBR
RDPAOPCS
SEQBPQDT
TFRCQREU
UGSDRSFV
VHTESTGW
WIUFTUHX
XJVGUVIY
YKWHVWJZ
ZLXIWXKA
AMYJXYLB
BNZKYZMC
COALZAND
```

```
AD   PBMYZ   M
bin  hxcfv   y...
bib  vm ei   i...
DP   BMYZM   C
```

```
DPBMYZMC
EQCNZAND
FRDOABOE
GSEPBCPF
HTFQCDQG
IUGRDERH
JVHSEFSI
KWITFGTJ
LXJUGHUK
MYKVHIVL
NZLWIJWM
OAMXJKXN
PBNYKLYO
QCOZLMZP
RDPAMNAQ
SEQBNOBR
TFRCOPCS
UGSDPQDT
VHTEQREU
WIUFRSFV
XJVGSTGW
YKWHTUHX
ZLXIUVIY
AMYJVWJZ
BNZKWXKA
COALXYLB
```

```
         .C  OAL.A  ND.LU  MBER.
MSG. 1  bln  hxcfv  yliet  azsoz  ...
MSG. 2  bib  vmoei  ipwvb  lwfgy  ...
         CO  AL.AN  D.LUM  BER.
```

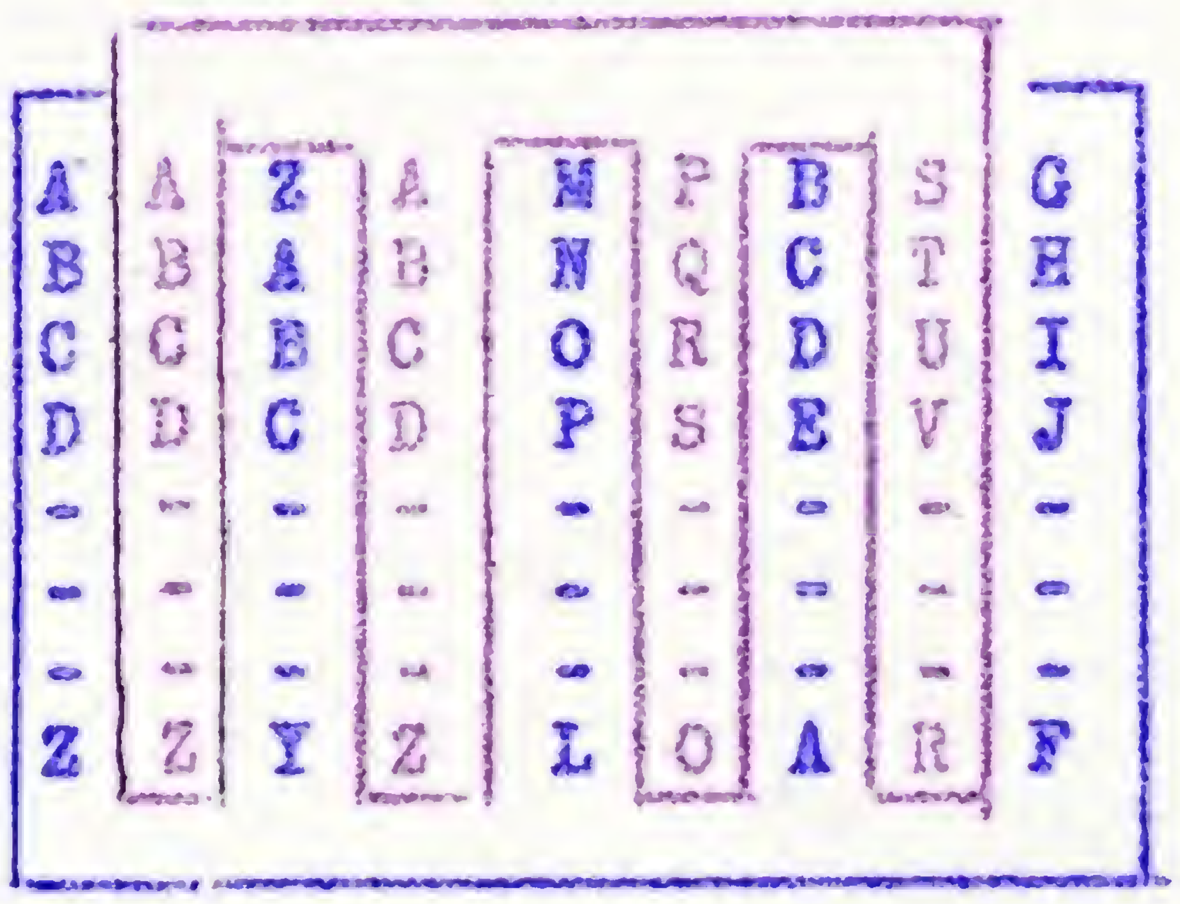
Figure 8.

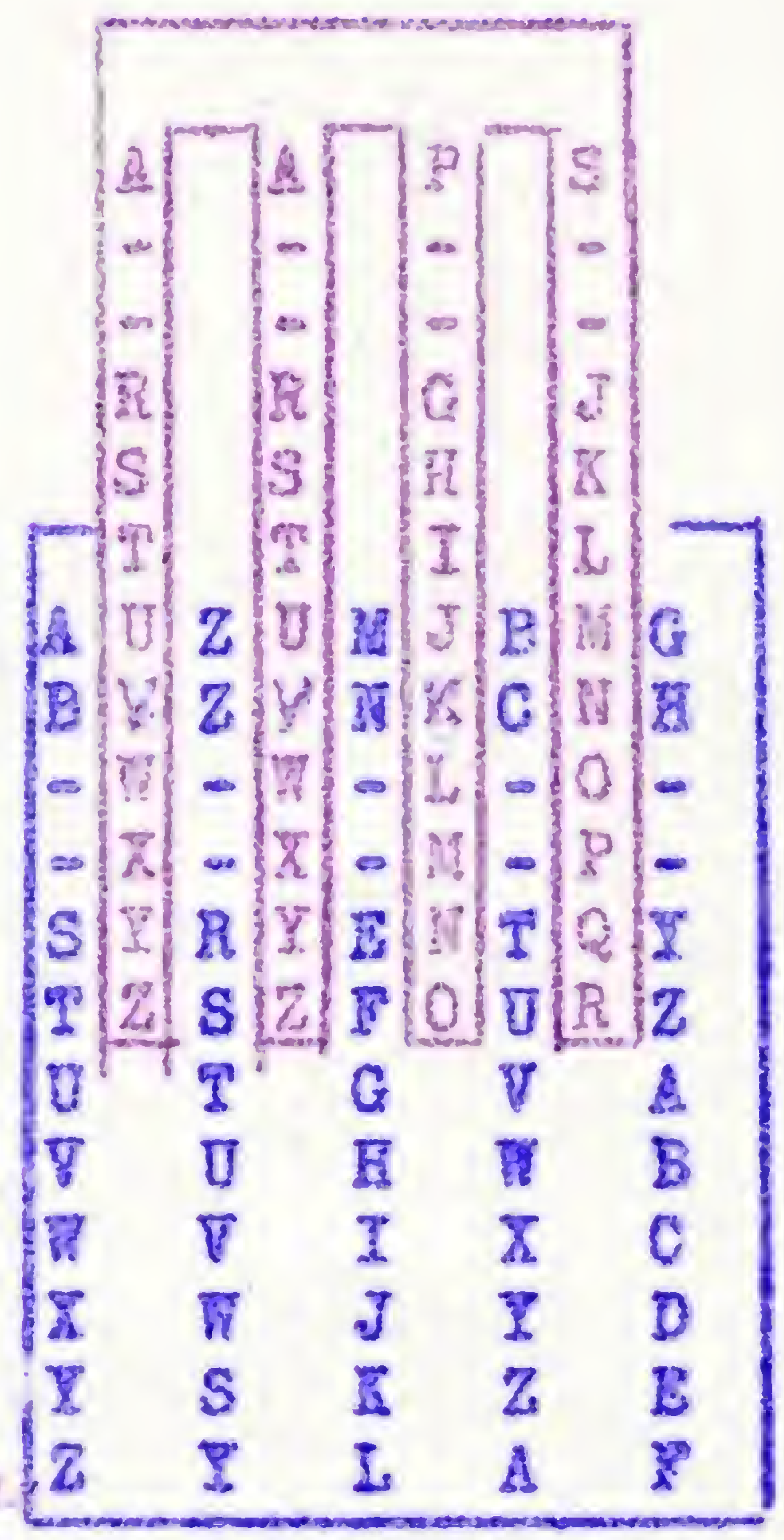
OFF-SET OF 2.

2 Msg. of 25.11.44
mmkof mqomm
2958 kHz

```
              .C   OAL.A  ND.LU  MBER.  AUTSS
MSG. 1   tttln  hxcfv  yliet  azsoz  kbqqj  wjrfi  pjkxe  dynoz  ...
MSG. 2   tttib  vmoei  ipwvb  lwfgv  qcrqw  huoaa  avulu  pibvu  ...
           CO   AL.AN  D.LUM  BER.A  UTSS

         AAZ   AMPBS
MSG. 1   kbqqj  wjrfi  ...
MSG. 2   qcrqw  huoaa  ...
         AAZAM  PB SG
```





```
           .   .AT.S  .FOUR  ..ONE  .ONE.  ZERO.  .
MSG. 1     z   kbqqj  wjrfi  pjkxe  dynoz  tdfxe  ...
MSG. 2     y   qcrqw  huoaa  avulu  pibvu  btxoz  ...
           A   T.S.F. OUR..  ONE.O  NE.XE  RO...
```

Figure 9.

TRIGRAPH-DIFFERENCES

2 MSG. of 26.10.44
ffacg nifus
2358 kHz

frequency

4495 · 1144

	00	00	17	13	25	00	13	00	.	.	.	
DIFFERENCE. MSG. 1	d	i	u	j	w	v	m	z	l	.	.	(35 B.)
MSG. 2	d	i	d	w	x	v	z	z	q	.	.	(65 B.)
	00	00	09	13	01	00	13	00	.	.	.	

700 · 3965 · 1037 · 4495

FREQUENCY

1144	700
4495	3965
...	4495
...	...
...	
18.282	35.838

$\times \frac{100}{33} =$ 55.400 108.600

$$\frac{55.400 + 108.600}{2} = 82.000$$

Figure 10.

MESSAGE IN PHASE.
SOLUTION

2 MSG. of 15.12.44
ccfbt tkiyu
4758 kHz

	COME.	IN.X.	ANSWE	R.IMM	EDIAT	ELY.R	RRRR.	REF.N
MSG. 1	lfojz	pikma	snusl	tzscb	wkliq	mprkc	zxtia	apnzj
MSG. 2	btgwq	tswfa	snjpm	koabl	woteh	rmyke	npprh	jskno
	MAURI	ENNE.	AND.D	ARANCE	E.SEC	TOR.P	D.VIS	IBILI

Q.AG.	FIVES	EVEN.	TO.SG	T.STE	ELE.C	LN.IS	.LAND
whsub	reyvr	dxdtx	gflrn	zzfan	caoyp	dsahm	ohkbp
ritap	kwbgk	nfwyk	raggu	dvyfw	cugxz	vgzcf	ckygz
TY.AL	MOST.	UNLIM	ITED.	PD.OV	ERCAS	T.AN	LIMIT
						(D)	

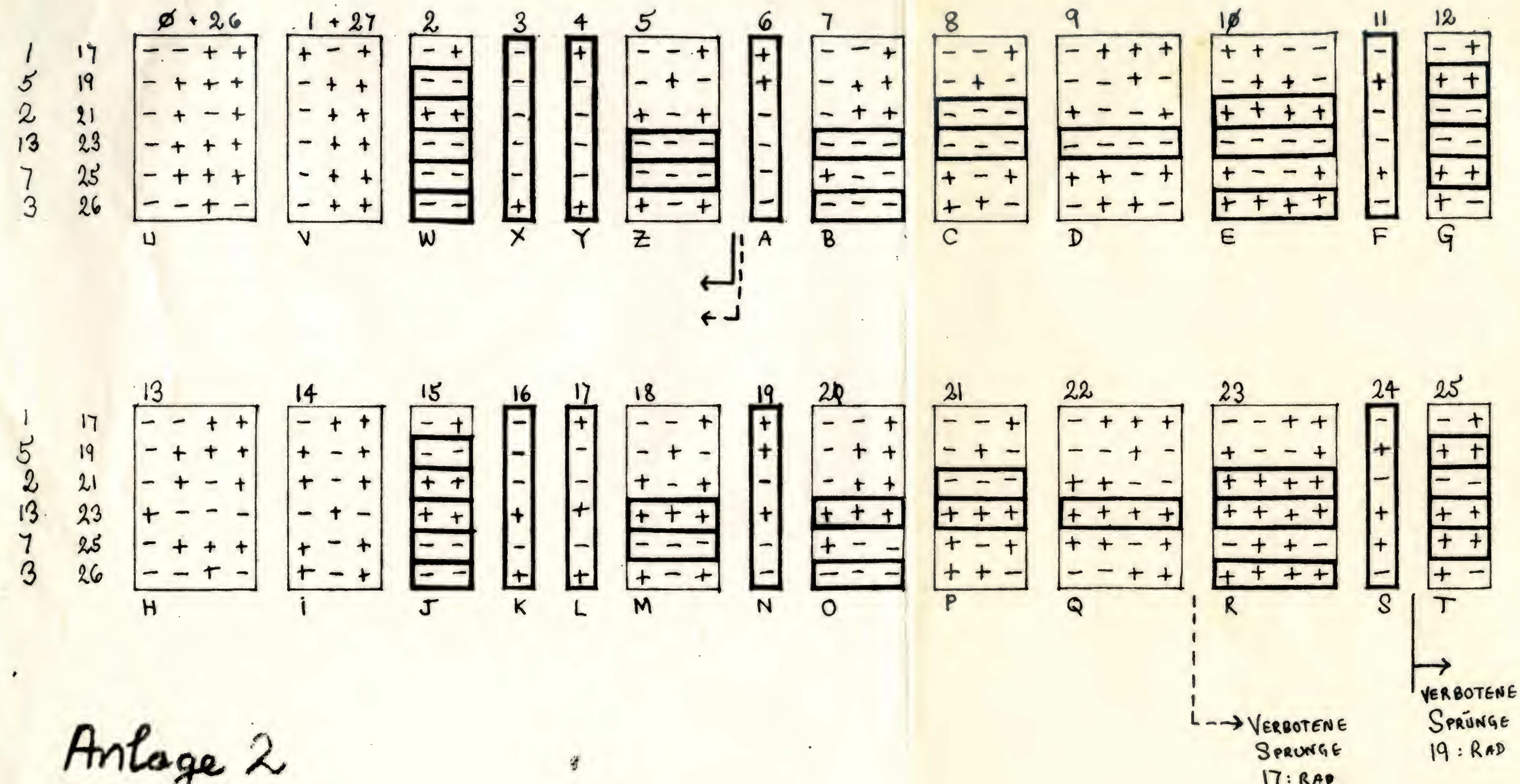
ING.F	IELD.	AND.W	EATHE	R.AT.	GRENO	BLE.S	UITAB
kfyhq	pofqz	nswxw	uptby	mvsts	mgkmk	wlvyw	psvtz
opfln	fkpln	fmbxk	lqtil	zhqmj	atphu	xdlgp	arfkr
ED.VI	SIBIL	ITY.I	N.TAR	ENTAI	SE.SE	CTOR.	JJJJJ

LE.FO	R.CUB	.CUB.	XXX.F	ROM.S	IG.OF	FICE.	XXX.P
ifyea	pyemv	brnar	waqur	tchuh	laysf	yhyln	wvmrg
urpqx	cidtc	osdkr	btspj	lraxl	ubqsy	ebnln	alsmr
.SITR	EP.NU	MBER.	SEVEN	..TWO	.FROM	.ONE.	THREE

LANE.	TO	
lagsz	ooxxx	
xbpfk	iymkm	.....
.ZERO	.EIGHT	

Figure 11.

TOP SECRET



Anlage 2

TOP SECRET

I

		~~27 26 23 20~~	~~14 13 10 7~~	~~26 25 22 19~~	~~13 12 9 6~~	~~23 22 18 15~~	~~10 9 5 2~~	~~22 21 17 14~~	~~9 8 4 1~~
		~~27 26 25 24~~	~~24 23 22 21~~	~~23 22 21 20~~	~~20 19 18 17~~	~~20 19 18 17~~	~~17 16 15 14~~	~~16 15 14 13~~	~~13 12 11 10~~
1	17	+ + + +	+ + + +	+ + + +	+ + + +	+ + + +	+ + + +	+ + + +	+ + + +
5	19	+ + + +	+ + + +	+ + + +	+ + + +	− − − −	− − − −	− − − −	− − − −
2	21	+ + + +	+ + + +	− − − −	− − − −	+ + + +	+ + + +	− − − −	− − − −
13	23	+ + + +	− − − −	+ + + +	− − − −	+ + + +	− − − −	+ + + +	− − − −
7	25	+ + − −	+ + − −	+ + − −	+ + − −	+ + − −	+ + − −	+ + − −	+ + − −
3	26	+ − + −	+ − + −	+ − + −	+ − + −	+ − + −	+ − + −	+ − + −	+ − + −

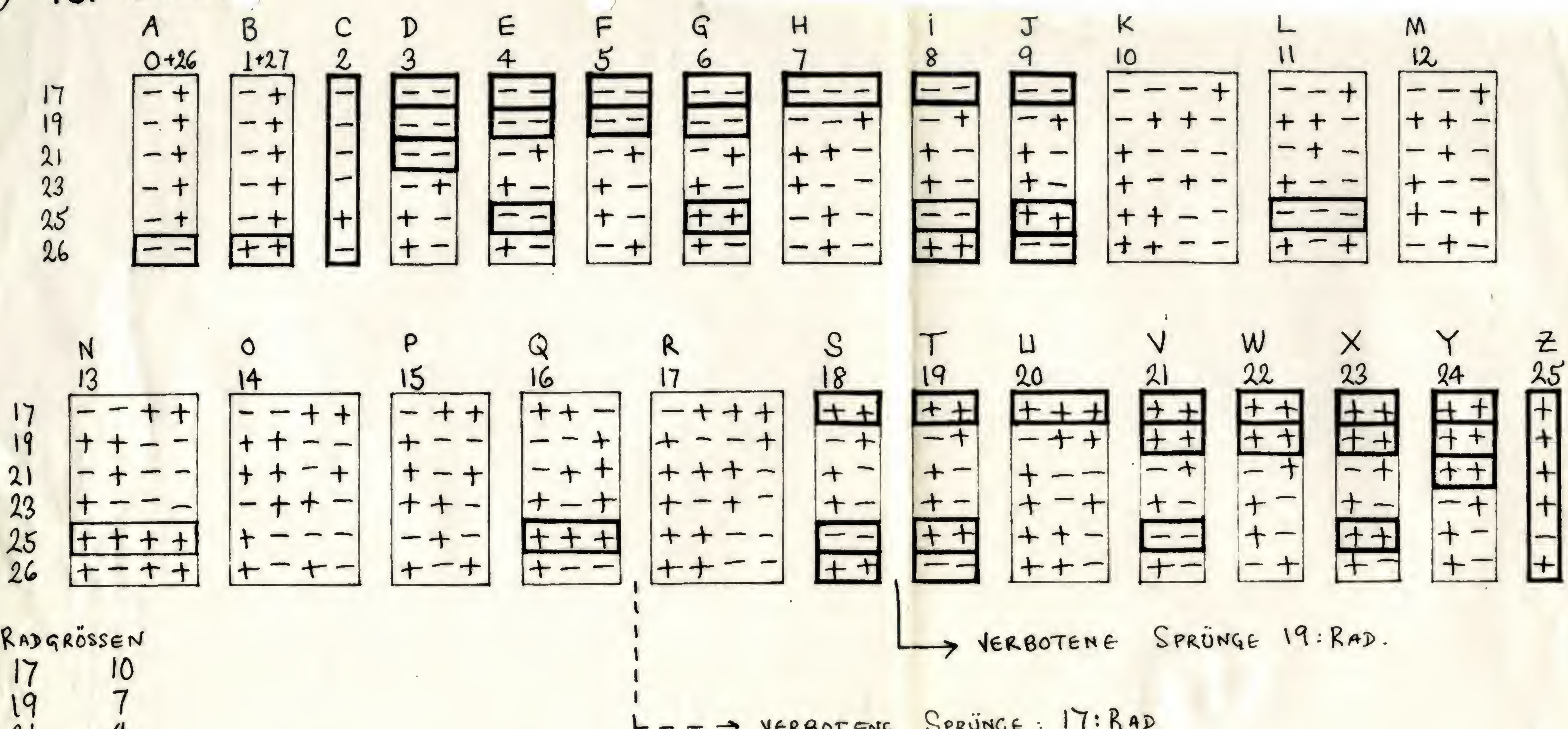
		~~27 26 23 20~~	~~14 13 10 7~~	~~25 24 21 18~~	~~12 11 8 5~~	~~23 22 18 15~~	~~10 9 5 2~~	~~21 20 16 13~~	~~8 7 3 0~~
		~~17 16 15 14~~	~~14 13 12 11~~	~~13 12 11 10~~	~~10 9 8 7~~	~~10 9 8 7~~	~~7 6 5 4~~	~~6 5 4 3~~	~~3 2 1 0~~
1	17	− − − −	− − − −	− − − −	− − − −	− − − −	− − − −	− − − −	− − − −
5	19	+ + + +	+ + + +	+ + + +	+ + + +	− − − −	− − − −	− − − −	− − − −
2	21	+ + + +	+ + + +	− − − −	− − − −	+ + + +	+ + + +	− − − −	− − − −
13	23	+ + + +	− − − −	+ + + +	− − − −	+ + + +	− − − −	+ + + +	− − − −
7	25	+ + − −	+ + − −	+ + − −	+ + − −	+ + − −	+ + − −	+ + − −	+ + − −
3	26	+ − + −	+ − + −	+ − + −	+ − + −	+ − + −	+ − + −	+ − + −	+ − + −

	17	19	21	23	25	26
17	/	−	1	−	−	−
19		/	−	−	1	−
21			/	−	−	−
23				/	−	−
25					/	2
26						/

← KOPPLUNGEN

Anlage 2a

II TOP SECRET



RADGRÖSSEN

17	10
19	7
21	4
23	3
25	2
26	1

BEISPIEL KORREKT

TOP SECRET

TOP SECRET

CORRECTIO. TO PAGE II O. ANLAGE 2-A

BLOCK N-13 OUGHT TO BE.

	N 13			
17	+	−	+	+
19	−	+	−	−
21	+	+	−	−
23	−	−	−	+
25	+	+	+	−
26	+	−	+	−

AND AS SUCH WOULD NOT HAVE ANY WHEEL CONSTANT FOR THIS VALUE. ERROR ON THE PART OF THE ORIGINATOR.

TOP SECRET

1) Abs. Einstellg. v. 9.12.44 für ll üoa fsc ür

A: 26er Rad bei c
25 " " " i
23 " " " k
21 " " " a
19 " " " k
17 " " " f

2) Fehler im Telefonat v. 24.12.44 betr. rel. Einstellg. v. 9.12.44 ür
26er Rad: p muß inaktiv sein, nicht wie durchgesprochen aktiv!

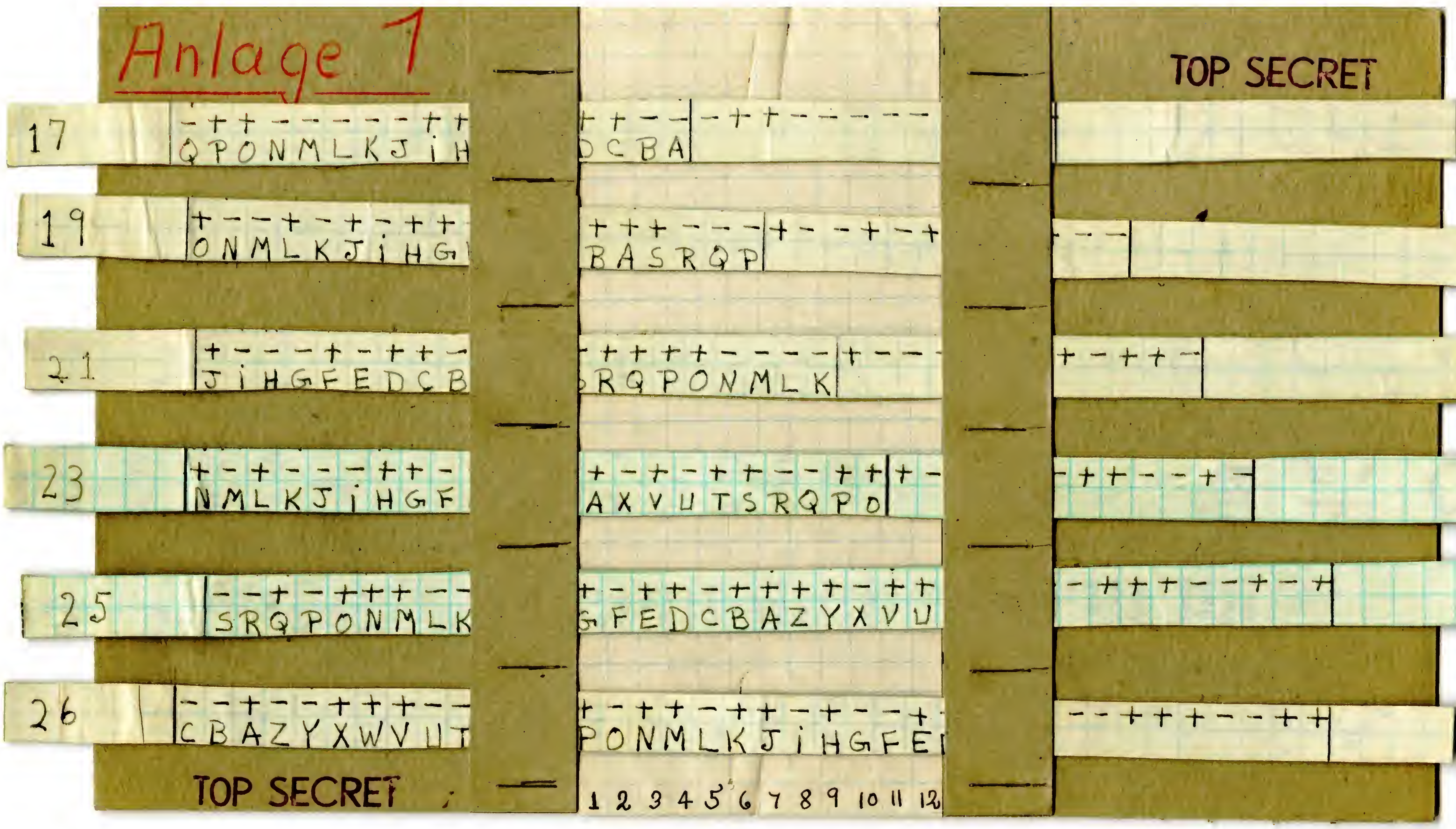
Datum	Kenngruppe	Frequenz	Erstellt von rel	abs.		
10.1.45	aa jog jkc ft	3665	Kdr.5	Kdr.5	24/23.1.45 (tel.) FS)	(21)
28.1.45	pp tūg amn pp	1870	Kdr.7	16	FS. v. 29.1. / 10.2.45	(22)
8.2.45	gg kjm gkā gg	3138	16	16	10.2./11.2.45	(23)
18.2.45	kk zxi srd kk	2061	EZ	16	19.2./20.2.45	
14.2.45	dd ubm εfj εy	3380	16	16	24.2.45	
19.2.45	tt oam jbi rp	4480	EZ	16	26.2./28.2.45	
27.2.45	ll obl tjq pl	2056	Kdr.6	16	27.2./28.2.45	
20.2.45	bb ūzh fod vz	2438	16	16	27.2./1.3.45	
16.2.45	ww gmi sro ww	3495	16	16	25.2./2.3.45	
25.2.45	gg kgk cεg to	2650	16	16	11.3./16.3.45	
1.3.45	rr igk fbj px		Luftwaffe	16	4.3./4.3.45	
3.3.45	ūū rit bfε ūū	2364	Kdr.6	16	4.3./5.3.45	
8.3.45	tt ico ria tv	27.25	16	— x)	19.3./ x)	
7.3.45	tt εrg εnn tl	2640	EZ	— x)	21.3./ x)	
13.3.45	kk bik aig zv	2730	16	16	17.3./9.4.45	
21.3.45	bb ūbf tfi aw	2630	16	16	24.3./25.3.45	
8.3.45	hh εkf gfj tl	2630	16	16	15.4./17.4.45	
22.3.45	vv rxm kph vv	2575	16	16	20.4./22.4.45	

x) keine „absolute" erstellt, da kein Spruchmaterial vorhanden. Schm.

Lfd. Nr.	Datum	Kenngruppe	Frequenz	Erstellt von rel.	absol.	
	1. 8. 44	bb krd igh jε	4 020	16		
	10. 8. 44	gg abc dεf ka	4 160	16	16	
	15. 8. 44	xx mxb gpd va	3 835	16	16	23.10.44
	21. 8. 44	ūū hcj nol ūū	4 285	Kdr. 7	16	30. 8. 44
	28. 8. 44	nn chg jcc bw	3 422	16	16	5. 9. 44
	31. 8. 44	rr gkl ojm rr	3 010	16	16	4. 9. 44
	3. 9. 44	cc fri gpm cc	3 295	16	16	17. 10. 44
	3. 9. 44	bb axm fpε aū	3 710	16	16	6. 9. 44
	8. 9. 44	dt		Kdr. 7	Kdr. 7	10. 10. 44
	9. 9. 44	jj acf cfo sb	3 240	16	16	
	9. 9. 44	cc sεg sma εy	3 590	16	16	9. 10. 44
	12. 9. 44	pp cfj cgf ūh	3 240	16	16	
	14. 9. 44	mm fūb ggn mm	3 295	16	16	
	14. 9. 44	dd gci εεg εd	3 665	16	16	17. 11. 44
	15. 9. 44	bb rit gai hr	2 330	Kdr. 5; 16	Kdr. 5	11. 10. 44
	15. 9. 44	cc yog ūdε by		Kdr. 5	Kdr. 5	
	16. 9. 44	bb cfc dcε ft		Kdr. 5	16	9. 10. 44
	16. 9. 44	bb imb ūmh xz	2 285	16	16	2. 10. 44
	16. 9. 44	cc εat dcb gt	3 280	16	16	30. 9. 44
	19. 9. 44	ct		Kdr. 5	Kdr. 5	
	21. 9. 44	mm dkg hgc mm	2 390	16	16	7. 10. 44
	24. 9. 44	aa xln pao ws	3 055	16	16	5. 10. 44
	25. 9. 44	ff dis mop xr		Kdr. 5	Kdr. 5	Meldg. v. 8.10.44
	25. 9. 44	dd ajn fεm ys		Kdr. 5	Kdr. 5	" " 5.10.44
	26. 9. 44	cc mεc ing ah		Kdr. 5	Kdr. 5	" " 6.10.44
	27. 9. 44	nn wyj jeg hp		16	16	14. 10. 44
	29. 9. 44	dd cdε agf vc	2 896	16	16	30. 11. 44
	3. 10. 44	mm jpn pch pa		Kdr. 5	Kdr. 5	Meldg. v. 4./7.10.44
	4. 10. 44	aa dla dla ap		Kdr. 5	Kdr. 5	" " 8.10.44
	6. 10. 44	gg dra gon xf	2 255	Kdr. 5	Kdr. 5	" " 15.10.44
	10. 10. 44	aa daε hεb wo		Kdr. 5	Kdr. 5	" " 13./14.10.44
	16. 10. 44	dd yza jso dd	2 958	16	16	2. 11. 44
	30. 10. 44	bb bga djj po	2 251	16	16	16. 11. 44
	14. 10. 44	ya	4 155	Beuteschlüssel		
	15. 10. 44	zb	4 155	Beuteschlüssel		

Lfd. Nr.	Datum	Kenngruppe	Frequenz	Erst[...] von rel.	abs.		
	1. 11. 44	xx hon lmo xx	3 450	16	16	15. 11. 44	
	1. 11. 44	oo cng hdh dp	2 256	16	16	21. 11. 44	
	2. 11. 44	up		Kdr. 5	Kdr. 5	Meldg. v. 7. 11. 44	
	3. 11. 44	ib		Kdr. 5	Kdr. 5	" " 8. 11. 44	
	6. 11. 44	hl		Kdr. 5	Kdr. 5	" " 9. 11. 44	
	6. 11. 44	gt		Kdr. 5	Kdr. 5	" " 13. 11. 44	
	10. 11. 44			16; Kdr. 5	Kdr. 5		
	10. 11. 44	ii dlf coj bm	1976	16	16	19. 11. 44	
	14. 11. 44	qq ezd mbh xz		Kdr. 5	Kdr. 5		
	15. 11. 44	gg ybl nab pg		Kdr. 5	Kdr. 5		
	15. 11. 44	gg ifj dnb hh	1825	16	16	25. 11. 44	
	21. 11. 44	ll fmu clo gt		Kdr. 5	Kdr. 5		
	23. 11. 44	gg nmh lkb sl		Kdr. 5	Kdr. 5		
	25. 11. 44	mm kof mgo mm	2 958	Kdr. 7	16	F.S. vom 28.11./30.11.44	
	27. 11. 44	hh ngr dvd ws		Kdr. 5	Kdr. 5	Meldg. vom 29. 11. 44	
	21. 11. 44	aa ert gpe ap	3 226	16	16	Fk. 2./3. 12. 44	
	18. 11. 44	bb alj lpl hg	3 226	16	16	Fk. 4./5. 12. 44	
	24. 11. 44	kk jzb hal yz	3 226	16/Kdr. 5	Kdr. 5	6. 12. 44	
	25. 11. 44	aa kgk cnn df	3 226	16	16	19./21. 12. 44	(3)
	24. 11. 44	ll pto gpd je	3 240	Kdr. 5		26. 11. 44	
	26. 11. 44	nn sgi roc ct		Kdr. 4	Kdr. 4	F.S. v. 13. 1. 45	(12)
	4. 12. 44	ll pnr gob wn		Kdr. 5	Kdr. 5	Meldg. v. 12. 12. 44	(1)
	4. 12. 44 x)	mm epp mrb rm	1985	Kdr. 5	Kdr. 5	" " 17. 12. 44	(2)
	15. 12. 44	cc ftb tki yu	4 758	16	16	19./28. 12. 44	(4)
	18. 12. 44	ll adf bgj ll	3 380	16	16	21./21. 12. 44	(5)
	21. 12. 44	?	2 700	Kdr. 7	Kdr. 7	F.S. v. 22. 12. 44	(6)
	23. 12. 44	rr sxp lgb an		Kdr. 5	Kdr. 5	Meldg. v. 26. 12. 44	(7)
	3. 12. 44	uh		Kdr. 5	Kdr. 5	" " 22. 12. 44	(8)
	9. 12. 44	ll uoa fsc ur	1800, 1950	Kdr. 6	16	Tel. v. 20.12.44 / 1. 1. 45	(9)
	15. 12. 44	zb	4 155	Bu.[illegible]		s. auch 15. 10. 44	
	20. 12. 44	jj goc irc bn	1986	16	16	11./12. 1. 45	(11)
	11. 12. 44	cc jna dec to		Kdr. 4	Kdr. 4	F.S. v. 13. 1. 45	(13)
	24. 12. 44	oo nov gpp wr	2 170	16	16	10./15. 1. 45	(15)
	12. 12. 44	aa hgo qpj fw	2 755	16	16	13./18. 1. 45	(16)
	1. 1. 45 xx)	mm vzg erh mm	3 400	16	16	9./10. 1. 45	(10)
	6. 1. 45	mm eps umk sg	5 430	16	16	14./15. 1. 45	(14)
	13. 1. 45	bb zhl aei bb	2 060	Kdr. 5	16	21./22. 1. 45	(17)
	24. 1. 45	cc out [illegible] bb	2 575	"	16	25./26. 1. 45	(1[illegible])
	15. 1. 45	pp igm ekd wk	2 685	"	16	18./26. 1. 45	(1[illegible])
	21. 1. 45	tt eix mlb tt	2 460	"	16	25./27. 1. 45	([illegible])

xx) gilt auch für 30.12., 31.12., 1., 2., 3. – 5.1. 12⁰⁰ Uhr [illegible].
x) gilt auch vom 1. – 9. 12. 44 [illegible] (Kdr. [illegible]) v. Kdr. 5.


Anlage 1
TOP SECRET
17
QPONMLKJiH
DCBA
19
ONMLKJiHG
BASRQP
21
JiHGFEDCB
SRQPONMLK
23
NMLKJiHGF
AXVUTSRQPO
25
SRQPONMLK
GFEDCBAZYXVU
26
CBAZYXWVUT
PONMLKJiHGFE
TOP SECRET
1 2 3 4 5 6 7 8 9 10 11 12

TOP SECRET

Verbotene und erlaubte Sprünge:

25 · Rad:

−	+
−	−
+	+
−	−

verboten:

−	−
−	−

erlaubt:

+	+	−
+	−	+

23 · Rad:

−	+	+	−	+	−
−	−	−	−	−	+
+	+	−	+	+	−

verboten:

−	−	−	−	−	−
−	−	−	−	−	−
−	−	+	+	+	−

erlaubt:

+	+	+	+	−	−
+	+	−	−	+	+
+	−	+	−	+	−

21 · Rad:

+	−	+	−	+	−	+	−	−	+
+	+	−	−	−	−	−	−	+	−

verboten:

+	+	−	+	+	−	−	+	−	+
+	+	−	−	−	−	−	−	−	−
+	+	−	−	−	−	−	−	−	−
+	+	−	−	−	+	+	+	−	+

erlaubt:

+	+	+	+	+	−	−	−	−	−	−
+	+	+	−	−	+	+	+	+	−	−
+	−	−	+	+	+	+	−	−	+	+
−	+	−	+	−	+	−	+	−	+	−

Anlage 3

TOP SECRET

TOP SECRET

	A	B	C	D	E	F	G	H	i	J	K	L	M	N	O	P	Q	R	S	T	Ü	V	W	X	Y	Z	
A	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	A
B	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	B
C	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	C
D	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	D
E	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	E
F	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	F
G	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	G
H	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	H
i	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	i
J	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	J
K	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	K
L	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	L
M	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	M
N	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	N
O	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	O
P	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	P
Q	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Q
R	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	R
S	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	S
T	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	T
Ü	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Ü
V	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	V
W	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	W
X	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	X
Y	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	Y
Z	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	Z
	A	B	C	D	E	F	G	H	i	J	K	L	M	N	O	P	Q	R	S	T	Ü	V	W	X	Y	Z	

Sprüngtabelle

(für AM 1)

Anlage 4

TOP SECRET

AWH

A	+	+	-	-	-
B	+	-	-	+	+
C	-	+	+	+	-
D	+	-	-	+	-
E	+	-	-	-	-
F	+	-	+	+	-
G	-	+	-	+	+
H	-	-	+	-	+
I	-	+	+	-	-
J	+	+	-	+	-
K	+	+	+	+	-
L	-	+	-	-	+
M	-	-	+	+	+
N	-	-	+	+	-
O	-	-	-	+	+
P	-	+	+	-	+
Q	+	+	+	-	+
R	-	+	-	+	-
S	+	-	+	-	-
T	-	-	-	-	+
U	+	+	+	-	-
V	-	+	+	+	+
W	+	+	-	-	+
X	+	-	+	+	+
Y	+	-	+	-	+
Z	+	-	-	-	+
[illegible]	-	+	-	+	-
[illegible]	-	+	-	-	-
8	+	+	+	-	+
9	-	-	+	-	-
+	+	+	-	+	+
/	-	-	-	-	-

ϕ	-	-	-	-	-	/	Blank
1	-	-	-	-	+	T	
2	-	-	-	+	-	3	Carriage Rt
3	-	-	-	+	+	O	
4	-	-	+	-	-	9	Space
5	-	-	+	-	+	H	
6	-	-	+	+	-	N	
7	-	-	+	+	+	M	
8	-	+	-	-	-	4	Line Feed
9	-	+	-	-	+	L	
10	-	+	-	+	-	R	
11	-	+	-	+	+	G	
12	-	+	+	-	-	I	
13	-	+	+	-	+	P	
14	-	+	+	+	-	C	
15	-	+	+	+	+	V	
16	+	-	-	-	-	E	
17	+	-	-	-	+	Z	
18	+	-	-	+	-	D	
19	+	-	-	+	+	B	
20	+	-	+	-	-	S	
21	+	-	+	-	+	Y	-
22	+	-	+	+	-	F	
23	+	-	+	+	+✓	X	-
24	+	+	-	-	-	A	
25	+	+	-	-	+	W	
26	+	+	-	+	-	J	
27	+	+	-	+	+	+	Fig.
28	+	+	+	-	-	U	
29	+	+	+	-	+	Q	-
30	+	+	+	+	-	K	
31	+	+	+	+	+	8	- Ltrs

1 2 3 4 5 6 7 8 9 0

Q W E R T Y U I O P

ϕ: - -

12: - +

17: + -

29: + +

1 SIGN

1

+	•	•	•	•	A	B	D	E	F	J	K	Q	S	U	W	X	Y	Z	8	+
-	•	•	•	•	C	G	H	I	L	M	N	O	P	R	T	V	3	4	9	/

2

•	+	•	•	•	A	C	G	I	J	K	L	P	Q	R	U	V	W	4	8	+
•	-	•	•	•	B	D	E	F	H	M	N	O	S	T	X	Y	Z	3	9	/

3

•	•	+	•	•	C	F	H	I	K	M	N	P	Q	S	U	V	Y	X	8	9
•	•	-	•	•	A	B	D	E	G	J	L	O	R	T	W	Z	3	4	+	/

4

•	•	•	+	•	B	C	D	F	G	J	K	M	N	O	R	V	X	3	8	+
•	•	•	-	•	A	E	H	I	L	P	Q	S	T	U	W	Y	Z	4	9	/

5

•	•	•	•	+	B	G	H	L	M	O	P	Q	T	V	W	X	Y	Z	8	+
•	•	•	•	-	A	C	D	E	F	I	J	K	N	R	S	U	3	4	9	/

2 SIGN

12

+	+	•	•	•	A	J	K	Q	U	W	B	+
+	-	•	•	•	B	D	E	F	S	X	Y	Z
-	+	•	•	•	C	G	I	L	P	R	V	4
-	-	•	•	•	H	M	N	O	T	3	9	/

13

+	•	+	•	•	F	K	Q	S	U	X	Y	8
+	•	-	•	•	A	B	D	E	J	W	Z	+
-	•	+	•	•	C	H	I	M	N	P	V	9
-	•	-	•	•	G	L	O	R	T	3	4	/

14

+	•	•	+	•	B	D	F	J	K	X	8	+
+	•	•	-	•	A	E	Q	S	U	W	Y	Z
-	•	•	+	•	C	G	M	N	O	R	V	3
-	•	•	-	•	H	I	L	P	T	4	9	/

15

+	•	•	•	+	B	Q	W	X	Y	Z	8	+
+	•	•	•	-	A	D	E	F	J	K	S	U
-	•	•	•	-	G	H	L	M	O	P	T	V
-	•	•	•	+	C	I	N	R	3	4	9	/

23

•	+	+	•	•	C	I	K	Q	P	U	V	8
•	+	-	•	•	A	G	J	L	R	W	4	+
•	-	+	•	•	F	H	M	N	S	X	Y	9
•	-	-	•	•	B	D	E	O	T	Z	3	/

24

•	+	•	+	•	C	G	J	K	R	V	8	+
•	+	•	-	•	A	I	L	P	Q	U	W	4
•	-	•	+	•	B	D	F	M	N	O	X	3
•	-	•	-	•	E	H	S	T	Y	Z	9	/

25

•	+	•	•	+	G	L	P	Q	V	W	8	+
•	+	•	•	-	A	C	I	J	K	R	U	4
•	-	•	•	+	B	H	M	O	T	X	Y	Z
•	-	•	•	-	D	E	F	N	S	3	9	/

34

•	•	+	+	•	C	F	K	M	N	V	X	8
•	•	+	-	•	H	I	P	Q	S	U	Y	9
•	•	-	+	•	B	D	G	J	O	R	3	+
•	•	-	-	•	A	E	L	T	W	Z	4	/

35

•	•	+	•	+	H	M	P	V	Q	X	Y	8
•	•	+	•	-	C	F	I	K	N	S	U	9
•	•	-	•	+	B	G	L	O	T	W	Z	+
•	•	-	•	-	A	D	E	J	R	3	4	/

45

•	•	•	+	+	B	G	M	O	V	X	8	+
•	•	•	+	-	C	D	F	J	K	N	R	3
•	•	•	-	+	H	L	P	Q	T	W	Y	Z
•	•	•	-	-	A	E	I	S	U	4	9	/

3 SIGNS

123

+	+	+	.	.	K	Q	U	8
+	+	-	.	.	A	J	W	+
+	-	+	.	.	F	S	X	Y
+	-	-	.	.	B	D	E	Z
-	+	+	.	.	C	I	P	V
-	+	-	.	.	G	L	R	4
-	-	+	.	.	H	M	N	9
-	-	-	.	.	O	T	3	/

124

+	+	.	+	.	J	K	8	+
+	+	.	-	.	A	Q	U	W
+	-	.	+	.	B	D	F	X
+	-	.	-	.	E	S	Y	Z
-	+	.	+	.	C	G	R	V
-	+	.	-	.	I	L	P	4
-	-	.	+	.	M	N	O	3
-	-	.	-	.	H	T	9	/

125

+	+	.	.	+	Q	W	8	+
+	+	.	.	-	A	J	K	U
+	-	.	.	+	B	X	Y	Z
+	-	.	.	-	D	E	F	S
-	+	.	.	+	G	L	P	V
-	+	.	.	-	C	I	R	4
-	-	.	.	+	H	M	O	T
-	-	.	.	-	N	3	9	/

234

.	+	+	+	.	Ç	K	V	8
.	+	+	-	.	I	P	Q	U
.	+	-	+	.	G	J	R	-
.	+	-	-	.	A	L	W	4
.	-	+	+	.	F	M	N	X
.	-	+	-	.	H	S	Y	9
.	-	-	+	.	B	D	O	3
.	-	-	-	.	E	T	Z	/

235

.	+	+	.	+	P	Q	V	8
.	+	+	.	-	C	I	K	U
.	+	-	.	+	G	L	W	-
.	+	-	.	-	A	J	R	4
.	-	+	.	+	H	M	X	Y
.	-	+	.	-	F	N	S	9
.	-	-	.	+	B	O	T	Z
.	-	-	.	-	D	E	3	/

245

.	+	.	+	+	G	V	8	-
.	+	.	+	-	C	J	K	R
.	+	.	-	+	P	L	Q	W
.	+	.	-	-	A	I	U	4
.	-	.	+	+	B	M	O	X
.	-	.	+	-	D	F	N	3
.	-	.	-	+	H	T	Y	Z
.	-	.	-	-	E	S	9	/

345

.	.	+	+	+	M	V	X	8
.	.	+	+	-	C	F	K	N
.	.	+	-	+	H	P	Q	Y
.	.	+	-	-	I	S	U	9
.	.	-	+	+	B	G	O	-
.	.	-	+	-	D	J	R	3
.	.	-	-	+	L	T	W	Z
.	.	-	-	-	A	E	4	/

134

+	.	+	+	.	F	K	X	8
+	.	+	-	.	Q	S	U	Y
+	.	-	+	.	B	D	J	-
+	.	-	-	.	A	E	W	Z
-	.	+	+	.	C	M	N	V
-	.	+	-	.	H	I	P	9
-	.	-	+	.	G	R	O	3
-	.	-	-	.	L	T	4	/

135

+	.	+	.	+	Q	X	Y	8
+	.	+	.	-	F	K	S	U
+	.	-	.	+	B	W	Z	-
+	.	-	.	-	A	D	E	J
-	.	+	.	+	H	M	P	V
-	.	-	.	-	C	I	N	9
-	.	-	.	-	G	L	O	T
-	.	-	.	-	R	3	4	/

4 SIGNS

1234

+	+	+	+	.	K	8
+	+	+	-	.	Q	U
+	+	-	+	.	J	+
+	+	-	-	.	A	W
+	-	+	+	.	F	X
+	-	+	-	.	S	Y
+	+	-	+	.	B	D
+	-	-	-	.	E	Z
-	+	+	+	.	C	V
-	+	+	-	.	P	I
-	+	-	+	.	G	R
-	+	-	-	.	L	4
-	-	+	+	.	M	N
-	-	+	-	.	H	9
-	-	-	+	.	O	3
-	-	-	-	.	T	/

1345

+	.	+	+	+	8	X
+	.	+	+	-	F	K
+	.	+	-	+	Q	Y
+	.	+	-	-	S	U
+	.	-	+	+	B	+
+	.	-	+	-	D	J
+	.	-	-	+	W	Z
+	.	-	-	-	A	E
-	.	+	+	+	M	V
-	.	+	+	-	C	N
-	.	+	-	+	H	P
-	.	+	-	-	9	/
-	.	-	+	+	G	O
-	.	-	+	-	R	3
-	.	-	-	+	L	T
-	.	-	-	-	4	/

OK
1245

+	+	.	+	+	8	+
+	+	.	+	-	J	K
+	+	.	-	+	Q	W
+	+	.	-	-	A	U
+	-	.	+	+	B	X
+	-	.	+	-	D	F
+	-	.	-	+	Y	Z
+	-	.	-	-	E	S
-	+	.	+	+	G	V
-	+	.	+	-	C	R
-	+	.	-	+	L	P
-	+	.	-	-	4	I
-	-	.	+	+	M	O
-	-	.	+	-	N	3
-	-	.	-	+	H	T
-	-	.	-	-	9	/

1235

+	+	+	.	+	8	Q
+	+	+	.	-	K	U
+	+	-	.	+	W	-
+	+	-	.	-	A	J
+	-	+	.	+	X	Y
+	-	+	.	-	F	S
+	-	-	.	+	B	Z
+	-	-	.	-	D	E
-	+	+	.	+	P	V
-	+	+	.	-	C	I
-	+	-	.	+	G	L
-	+	-	.	-	R	4
-	-	+	.	+	H	M
-	-	+	.	-	N	9
-	-	-	.	+	O	T
-	-	-	.	-	3	/

2345

.	+	+	+	+	8	V
.	+	+	+	-	C	K
.	+	+	-	+	P	Q
.	+	+	-	-	I	U
.	+	-	+	+	G	-
.	+	-	+	-	J	R
.	+	-	-	+	L	W
.	+	-	-	-	A	4
.	-	+	+	+	M	X
.	-	+	+	-	F	N
.	-	+	-	+	H	Y
.	-	+	-	-	S	9
.	-	-	+	+	B	O
.	-	-	+	-	D	3
.	-	-	-	+	[illegible]	Z
.	-	-	-	-	E	/

German Use of the Baudot Code

+ = Upper Case (same as typewriter shift key)

8 = Lower Case (shifting back after machine has been in upper case)

9 = Space

These three symbols are usually used twice or more consecutively.

3, 4, / are not used.

Upper case symbols:

Numbers are represented by the first row ~~at~~ the typewriter keyboard in upper case, i.e.,

1	2	3	4	5	6	7	8	9	0
Q	W	E	R	T	Y	U	I	O	P

Upper case M = period, or dit.
Upper case A = dash
Upper case K = open parentheses
Upper case L = close parentheses
Upper case V = some sort of spacer
Upper case S = apostrophe
Upper case SS = quotes

Frequently a string of N's indicate an error has been made, word will be reprinted.

Every time a number is given, i.e. ++WRT889, later in the message the numbers will be spelled out ZWO VIER FUENF.

Abbreviations will also be spelled out phonetically later in the message. If he gives call signs GNT, later GUSTAV NORDPOL THEODOR will appear.

Messages almost always begin ++ZZZ------88.

German Phonetic Alphabet:

ANTON
BERTA
CAESAR
DORA
EMIL
FRIEDRICH
GUSTAV
HEINRICH
IDA
JULIUS
KONRAD
LUDWIG
MARTHA
NORDPOL
OTTO
PAULA
QUELLE
RICHARD
SIEGFRIED
THEODOR
ULLRICH
VIKTOR
WILHELM (WILLI)
XANTHIPPE
YPERN
ZEPPELIN

German Numbers:

1. EINS
2. ZWO
3. DREI
4. VIER
5. FUENF
6. SECHS
7. SIEBEN
8. ACHT
9. NEUN
10. NULL